11. *Lunacek O.* Knowledge system new tool of the security experts education // 6th International Conference on Military Technologies. 2017. P. 430–434.

УДК 304.2+316.723

С. С. Лушникова
Научный руководитель: д-р пед. наук, проф. Л. В. Астахова
Южно-Уральский государственный университет, Челябинск

КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАРУБЕЖНЫХ И РОССИЙСКИХ ИССЛЕДОВАНИЙ

Аннотация. В данной статье произведен анализ литературы, посвященной информационной и кибербезопасности, изданной в период с 2010 года по настоящее время. Выделены основные аспекты содержания публикаций и методики исследований данной темы.

Ключевые слова: информационная безопасность; защита информации; культура информационной безопасности; киберкультура; осведомленность; кадровая безопасность; организационная культура; культура безопасности.

Согласно статистическим исследованиям, устойчивой тенденцией является тот факт, что более двух третей ущербов, имеющих злонамеренный характер, исходит от персонала предприятия [1]. Несмотря на то, что защита информационного капитала крайне важна для обеспечения стабильной экономики [2], а недоразвитость киберкультуры может привести к серьезному ущербу не только в экономической отрасли, но и пошатнуть безопасность целой нации [3], область культуры информационной безопасности и кибербезопасности, которая закладывает морально-этическую основу отношения человека к защите информации, до сих пор слабо изучена. Цель данной статьи — охарактеризовать результаты сравнительного анализа публикаций, появившихся во второе десятилетие XXI века, посвященных культуре информационной безопасности и культуре кибербезопасности в зарубежных и российских источниках, и показать их потенциальные возможности для развития практики защиты информации на предприятии.

Анализ был произведен при помощи базы данных Scopus. Исследовались статьи, найденные по запросу «Cybersecurity culture» OR «Information security culture» за временной промежуток с 2010 года по настоящий момент. Выбор данного отрезка времени обусловлен тем, что существующие обзоры литерату-

ры по этой тематике охватывают года не позднее 2013 года. Общее количество найденных публикаций на заданную тему — 85, во внимание были приняты заглавия, аннотации статей и ключевые слова.

Исследование призвано ответить на следующие вопросы: 1. Какую часть в процентном соотношении занимают российские публикации в рамках общего количества статей на заданную тему? 2. Какие аспекты данной тематики исследуются за рубежом и в России? 3. Какие исследовательские методы доминируют?

Данные Scopus демонстрируют следующую статистику распределения публикаций по странам. Наибольшее число публикаций имеют Южная Африка, (24 статьи), Австралия (12 статей), Малайзия (8 статей). В России же на заданную тематику опубликовано всего 2 статьи, что составляет 2,35 % от общего числа публикаций, и в 12 раз меньше, чем число статей ученых из Южной Африки.

Что касается аспектов, изучаемых в публикациях, посвященных теме культуры информационной безопасности, самое большое количество статей посвящено тематике взаимосвязи культуры информационной безопасности с культурой организационной и с культурой национальной (10,8 %). Следом идут публикации о методах измерения и оценки культуры информационной безопасности в организации (9,6 %). Также достаточно большое число статей посвящено исследованию существующей культуры информационной безопасности в какой-либо конкретной организации или группе организаций будь то библиотеки, учреждения здравоохранения, школы (8,4 %). Достаточно распространены аспекты, посвященные факторам, способствующим успешному функционированию культуры ИБ; управлению изменениями в культуре информационной безопасности, происходящими при каких-либо изменениях в режиме работы организации. Не последнее место занимает и тематика определения и рамок культуры ИБ, что свидетельствует о слабой развитости данной темы и отсутствии достаточного количества материала для теоретического фундамента знаний в этой области.

Впервые на проблему культуры информационной безопасности в России обратила Л. В. Астахова. Опираясь на функциональную концепцию культуры и сущность информационной безопасности, она определила концепт культуры безопасности информации как особый способ организации и развития информационной деятельности субъекта, который представлен в ценностно ориентированных моделях его информации, взаимодействие как отправителя и получателя информации, при котором он определяет и контролирует единство существования и развития информационных объектов в их познавательных и коммуникативных проявлениях [4]. А. Малюк и Н. Милославская рассмотрели гуманитарную проблематику культуры кибербезопасности, связанную с эти-

ческими вопросами развития информационных технологий. Они предлагают собственную, не основанную на западных аналогах, программу курса обучения кибербезопасности ИТ-специалистов, благодаря которой они должны будут иметь возможность формулировать и аргументировать свои предложения, убеждать высшее руководство организации в необходимости принятия мер по защите информации, чтобы иметь возможность работать с персоналом, и т. д. [5].

К сожалению, ввиду ограниченности доступа к материалу большей части исследований досконально проанализировать методы не удалось, но, согласно доступным материалам, превалирует методы исследования посредством интервьюирования и обзора литературы.

По полученным в ходе анализа результатам можно судить, что область культуры информационной безопасности очень интенсивно исследуется в зарубежных странах. Тем не менее зарубежные ученые считают, что набор тем и методов исследований крайне ограничен и носит по большей части теоретический характер, причем большинство теорий адаптировано из психологии, экономики, управленческих и других гуманитарных наук. Эмпирический анализ использовался только в одной пятой из всего количества материала. Это свидетельствуют о необходимости проведения дополнительных эмпирических исследований проблем и принципов культуры информационной безопасности [2]. Эти выводы позволили зарубежным ученым заключить, что данная область научных знаний носит еще только зарождающийся характер [6]. По их мнению, в будущем эта отрасль должна использовать методы, незадействованные ранее и подходы, которые в контексте культуры информационной безопасности еще не исследовались. В России эта актуальная проблема практически не изучена. Этот факт должен послужить хорошим стимулом к исследованию данной темы в ближайшем будущем. Потому как в нашей стране не предлагались ни какие-либо новые инструменты для оперирования киберкультурой на предприятии, не проводились исследования по оценке культуры информационной безопасности. Не затронуты темы влияния смежных культур на культуру ИБ, а также управления изменениями в этой области.

Исходя из результатов проведенного анализа, мы определили понятие КИБ и разработали организационно-документационную модель ее развития с целью дальнейшего применения в управлении этой сферой защиты информации на предприятии. Определение КИБ было уточнено на основе наиболее цитируемых определений, используемых ранее. **Культура информационной безопасности** — это такой способ организации информационной деятельности субъекта, при котором ценностные модели его поведения обеспечивают ему и другим субъектам безопасное функционирование и развитие в информационно-технологической среде.

Основой системы локальных организационно-распорядительных документов на предприятии служит «Стратегия развития культуры информационной безопасности» (далее — Стратегия), шаблон которой мы разработали в ходе нашего исследования. Документ содержит цели, задачи, направления и методы оценки и развития культуры ИБ.

Обязательным элементом документа является характеристика желаемого уровня развития КИБ по завершению реализации Стратегии. Уровень определяется на основе результатов текущей оценки состояния культуры информационной безопасности и заданного эталона ее уровня, который утверждается руководством организации и фиксируется в Стратегии.

Стратегия должна быть адаптирована к организационной культуре предприятия. Для своевременной реализации должны быть назначены ответственные и определена ответственность при несоблюдения пунктов Стратегии, что также фиксируется в документе.

На завершающем этапе формирования стратегии необходимо обеспечить хороший уровень коммуникаций между всеми заинтересованными сторонами и при окончательном утверждении осведомить персонал о принятии стратегии развития культуры информационной безопасности.

Таким образом, результаты предпринятого в ходе исследования сравнительного анализа российских и зарубежных публикаций, появившихся во второе десятилетие XXI века, посвященных культуре информационной безопасности и культуре кибербезопасности, обладают научной и практической значимостью. Они позволили выявить интенсивное развитие науки и практики развития КИБ за рубежом по сравнению с Россией. Этот вывод дал возможность определить перспективные направления, методы и формы ее развития в практике защиты информации на российских предприятиях, а также систему документационного обеспечения этого процесса.

Список литературы

1. *Астахова Л. В.* Проблема оценки HR-уязвимости объекта защиты информации // Вестн. УрФО безопасность в информационной сфере. 2011. № 1. С. 26–34.

2. *Alhogali A.*, *Mirza A.* Information Security Culture: A Definition and A Literature Review. URL: https://www.researchgate.net/publication/282754259_Information_Security_Culture_A_Definition_and_A_Literature_Review.

3. *Gcaza N.*, *von Solms R.* A strategy for a cybersecurity culture: A South African perspective // Electronic Journal of Information Systems in Developing Countries. 2017. № 80 (1). P. 1–17.

4. *Astakhova L. V.* The concept of the information-security culture // Scientific and Technical Information Processing. 2014. № 41(1). P. 22–28.

5. *Malyuk A.*, *Miloslavskaya N.* Cybersecurity culture as an element of IT professional training // 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications. DIPDMWC2016. 7529390. P. 205–210.

6. *Karlsson F.*, *Karlsson J.*, *A. M.* Information security culture — state-of-theart review between 2000 and 2013 // Information & Computer Security, Vol. 23. Iss 3. 2015. P. 246–285.

УДК 006.89

Л. М. Матвеенкова
Научный руководитель: д-р тех. наук, проф. В. Л. Кузнецов
Московский государственный технический университет
гражданской авиации, Москва

ПРОБЛЕМА ТЕРМИНОЛОГИИ В ОБЛАСТИ ОПЕРАЦИОННЫХ БАНКОВСКИХ РИСКОВ

Аннотация. Объектом исследования данной работы является понятийный аппарат в области операционных банковских рисков. Проблема риска является одной из ключевых концепций в финансовой деятельности, в связи с чем вопрос систематизации и классификации рисков является одним из наиболее актуальных. Анализ понятия операционного банковского риска, систематизация понятийного аппарата рассматриваемой предметной области осуществлялись с целью снятия существующих разногласий в понимании процесса управления операционными рисками.

Ключевые слова: операционный риск; внутренний банковский риск; внешний банковский риск; классификация видов операционного риска; риск операционного контроля.

Деятельностью банковских организаций являются финансовые средства и потоки. В связи с этим тесно переплетаются понятия финансового и банковского рисков. «Более того, насчитывается более 40 различных критериев рисков и более 220 видов рисков, так что в экономической литературе нет единого понимания в этом вопросе» [1].

Под «риском» принято понимать вероятность (угрозу) потери предпринимателем части своих ресурсов. Сущность риска состоит в возможности отклонения полученного результата от запланированного.